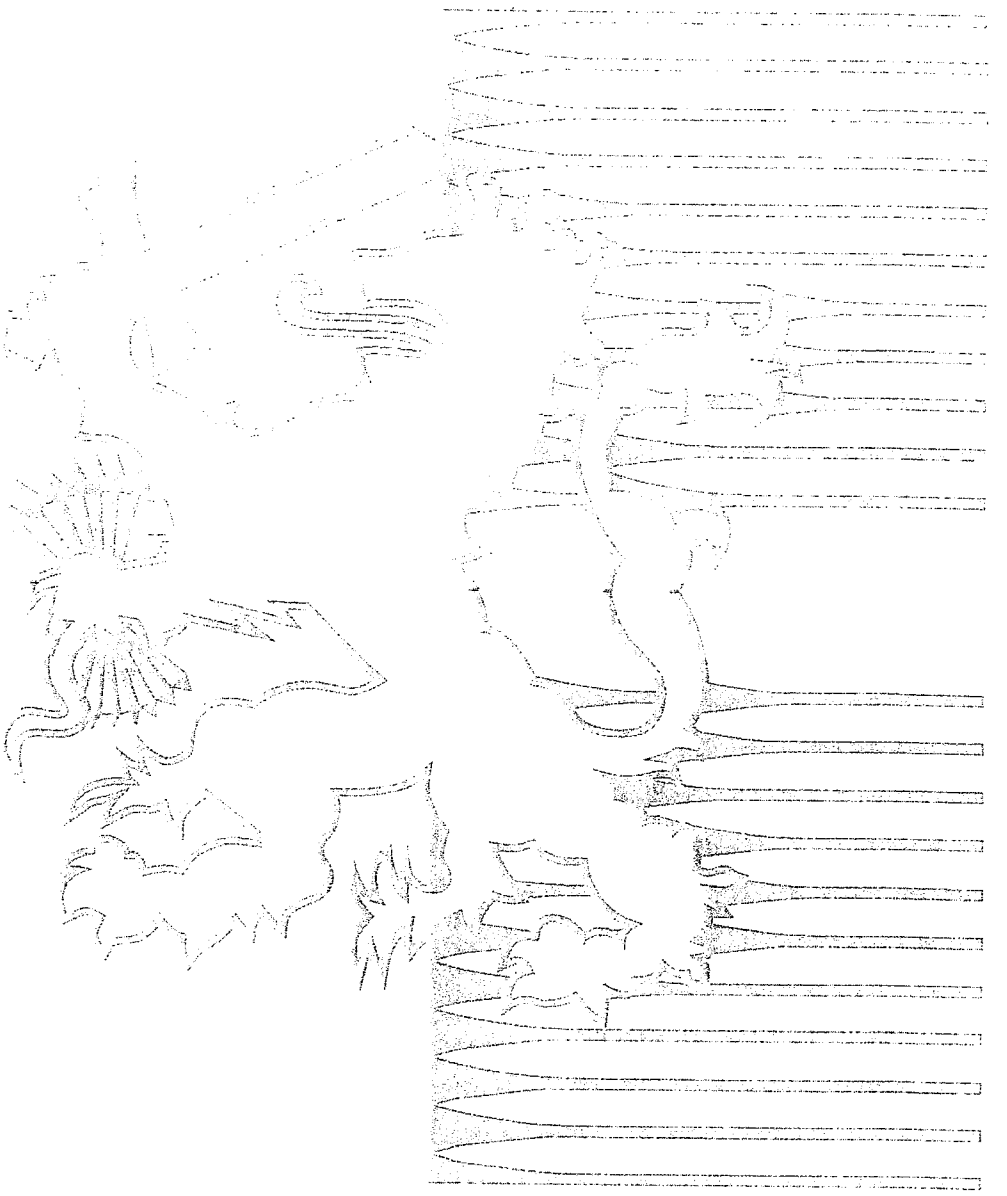
DIRECTIE OPERATIEN
KONINKLIJKE LANDMACHT

MAANDBERICHT JULI 1993



AFDELING INLICHTINGEN EN VEILIGHEID

MAANDBERICHT JULI 1993

Nummer: 0029375

Exemplaarnummer: 6

Het maandbericht is een uitgave van de Directie Operatiën Koninklijke landmacht, Afdeling Inlichtingen & Veiligheid, Sectie Veiligheid. Gerapporteerd wordt over ontwikkelingen, achtergronden en activiteiten in binnen- en buitenland die direct of indirect van invloed kunnen zijn op de militaire veiligheid van de Koninklijke landmacht.

Eventuele reacties op deze periodiek of suggesties ten behoeve van een volgend maandbericht kunt U richten aan:

Hfd Sie Veiligheid
MPC 16A
Postbus 96904
2509 JH Den Haag
t.a.v. CENTRALE STURING
tel.: 070-3281681

De inhoud van dit maandbericht is niet gerubriceerd en kan door U gebruikt worden als ondersteuning van aktiviteiten die de veiligheidszin binnen Uw ressort beogen te optimaliseren. Het is echter niet toegestaan de geboden informatie buiten de defensie-organisatie bekend te stellen.

U wordt verzocht de tot nu toe ontvangen geclassificeerde/gerubriceerde exemplaren van het maandbericht/MV-bericht uiterlijk 31 december 1993 te hebben geretourneerd aan:

Hfd Sie Veiligheid
MPC 16A
Facilitair Bedrijf
Bureau Naverwerking
Postbus 96904
2509 JH Den Haag

INHOUDSOPGAVE

HOOFDSTUK 1

ALGEMEEN

In dit maandbericht worden in de hoofdstukken 3 en 4 een tweetal aspecten betreffende computerbeveiliging nader belicht. Hoofdstuk 3 geeft een aantal aanwijzingen hoe zo veilig mogelijk gegevens op een portable computer kunnen worden verwerkt. Enerzijds is een portable computer diefstal-gevoelig, anderzijds kunnen verwerkte en/of opgeslagen gegevens een rubricering of merking hebben. Ook kan het zijn dat gegevens moeilijk of niet vervangbaar of reproduceerbaar zijn.

Hoofdstuk 4 betreft een steeds groter wordend risico, het computervirus. De subtitel van het hoofdstuk is kenmerkend voor de inhoud: "Hoe loop ik 95 procent minder kans op een besmetting met een computervirus".

HOOFDSTUK 2

ACTUEEL OVERZICHT VEILIGHEIDSINCIDENTEN

2.1 DE INCIDENTEN IN JULI 1993

Onder de meldingen van inbreuken op de militaire veiligheid bevonden zich in de maand juli weer meldingen betreffende de documentenveiligheid.

In een vernietigingsruimte voor gerubriceerde documenten werden na kantoortijd 5 Stg Confidentieel gerubriceerde documenten aangetroffen. Volgens de regelgeving dient de aanbieder van gerubriceerd afvalpapier tot en met de daadwerkelijke vernietiging aanwezig te zijn. Indien niet vernietigd kan worden, neemt men de te vernietigen documenten weer mee terug.

Totaal werd tijdens sluit- en/of controle-rondes 11 maal een kamer niet afgesloten aangetroffen. Meestal waren de bureauladen in deze kamers ook niet afgesloten. Er werd 6 maal een Stg Confidentieel en 1 maal een Stg Geheim gerubriceerd document in de niet afgesloten kamers aangetroffen. Verder werden Stg Confidentieel gerubriceerde documenten aangetroffen in een afvalbak, een papierbak voor ongerubriceerd papier en "gewoon" op de gang.

Een Stg Confidentieel gerubriceerd postpakket behoefde door de geadresseerde niet meer geopend te worden; zowel de binnen- als de buitenenveloppe waren reeds opengescheurd.

Sluit- en controle-rondes worden mede gelopen in het kader van materieelveiligheid. Zo werden in Kampen en Lopik diverse deuren van loodsen en andere ruimtes niet afgesloten aangetroffen. In Soesterberg werd tijdens een ronde geconstateerd dat een FAL op de vensterbank van de wapenonderhoudsruimte lag. Bij het betreden van het gebouw bleken meerdere deuren niet afgesloten te zijn.

Soesterberg werd de maand juli 3 maal geconfronteerd met een bommelding, 1 maal in Kamp Soesterberg en 2 maal in de DuMoulin-kazerne. In alle gevallen was er sprake van loos alarm.

Ondanks dat bommeldingen bij de Kl over het algemeen "loos alarm" blijken te zijn, moet een bommelding te allen tijde serieus worden genomen. Een blik in de kranten levert al gauw enig inzicht in de mogelijke uitwerking van een explosie. De mogelijk ernstige gevolgen rechtvaardigen een vast omlijnde benadering.

Knip-akties in Kl-hekken te Bergen op Zoom, Havelte en Vught leverden buiten de kapotte hekken geen vervolg-schade op.

Wat wel meervoudige schade opleverde waren inbraken in messes in Vught en Maastricht. Hierbij werden geld, sigaretten en snoep gestolen.

In 't Harde werd een YA 4440 ontvreemd en een dag later in Wezep weer teruggevonden. Diefstal in Keizersveer leverde een buit en dus een schade op van touwwerk, benzine en gereedschap.

Gevallen van (vermeende) verdachte belangstelling deden zich voor op een oefenterrein in de BRD en in Brunssum. Door oplettendheid en adequaat reageren van het personeel konden de personalia van de belangstellenden worden achterhaald.

Belangstelling voor een Kl-object kan vele redenen hebben. Combineren we belangstelling met een bommelding, dan geeft het gedrag van het personeel belangrijke informatie. Laconiek reageren op een bommelding (in plaats van gedisciplineerd handelen volgens de instructies) kan door de potentiele bommenlegger worden vertaald in een groter aantal slachtoffers. Een groot aantal slachtoffers van een bom waar notabene voor gewaarschuwd is levert buiten veel persoonlijk leed een deuk op in de geloofwaardigheid van het oordeelsvermogen van Kl-personeel.

2.2 VOORMALIG JOEGOSLAVIE

Twee dienstplichtige militairen hadden het voornemen op familiebezoek in respectievelijk Kroatië en Servië te gaan. Door één van de families werd gevraagd of het mogelijk was wapens en/of munitie te verkrijgen en mee te nemen. Betrokkene heeft e.e.a. gemeld aan zijn S2 en aangegeven hier niet op in te zullen gaan.

Zeven dienstplichtigen werden gerepatrieerd nadat zij bekend hadden drugs te hebben gebruikt. Vier van hen hadden zich vergrepen aan de lokale plantengroei. Deze planten groeiden in de buurt van hun HQ en zijn rond deze tijd rijp om te roken.

Eén van de drugs-gerepatrieerden was in het bezit van een (niet organiek) vuurwapen.

Een dienstplichtige werd gerepatrieerd nadat hij een aantal diefstallen had bekend.

Van een aantal NL militairen werd geconstateerd, dat zij meer dan zakelijke relaties met de lokale bevolking onderhielden. Door deze "innige" contacten met locals kan de neutraliteit van de VN t.o.v. de strijdende partijen in gevaar worden gebracht.

HOOFDSTUK 3

BEVEILIGING VAN PORTABLE COMPUTERS

Veel bedrijven en instellingen maken gebruik van portable computers. Ook bij de landmacht wordt gebruik gemaakt van deze computers. Een nadeel van de portables is evenwel, dat zij gemakkelijk ontvreemd kunnen worden. Dat kan als consequentie hebben dat vertrouwelijke gegevens in verkeerde handen terecht komen.

Welke maatregelen zijn te nemen om de gegevens op portable computers zoveel mogelijk te beveiligen?

Maatregelen

Het is belangrijk portables nooit onbeheerd achter te laten, ook niet in de bagageruimte van auto's. Een laptop is een gewild artikel voor veel mensen en de kleine crimineel zal dan ook altijd proberen een auto open te breken als hij weet dat er een portable computer in ligt. Tevens wordt voorkomen dat de computer schade oploopt door temperatuurwisselingen die kunnen optreden.

Ook met het onbeheerd achter laten van een draagbare computer in een hotelkamer worden onnodige risico's genomen. Bedenk dat veel mensen tegenwoordig met een computer kunnen omgaan, daarnaast is het betrekkelijk eenvoudig om snel een kopie te maken van gegevens die zich op de harddisk bevinden.

Tevens is het noodzakelijk het opstarten van de computer in enigerlei vorm te beveiligen. Sommige portables zijn uitgerust met een zogenaamde beveiligingschip. Daarmee kan worden afgedwongen dat -iedere keer dat de computer wordt aangezet- een wachtwoord moet worden ingevoerd. Dit is geen complete beveiliging. In veel gevallen is na het verwijderen van een klein batterijtje deze chip uitgeschakeld. Een andere mogelijkheid is het verwijderen van de harde schijf en deze aansluiten op een andere computer.

Een andere vorm van beveiligen is het gebruik maken van beveiligings-programmatuur, waarmee het opstarten beveiligd kan worden. Deze programmatuur biedt ook vaak faciliteiten voor het versleutelen van opgeslagen gegevens (encrypten).

Het versleutelen van gegevens kost overigens tijd, vooral als daarvoor gebruik wordt gemaakt van software. In de praktijk blijkt encryptie daardoor moeilijk geaccepteerd te worden.

Gegevens op diskette

Indien alle bovengenoemde maatregelen niet mogelijk zijn, dan rest feitelijk nog maar één oplossing: alleen programmatuur opslaan op de vaste schijf en geen gegevens. De gegevensbestanden worden dan vastgelegd op een diskette. De diskettes dienen na het gebruik op een veilige plaats opgeborgen te worden.

Sommige programma's kunnen echter niet of slechts moeizaam werken zonder gebruik te maken van de vaste schijf voor het gebruik van gegevens bestanden. Dat zou betekenen dat na gebruik alle gegevens van de harddisk gekopieerd moeten worden naar een diskette en dat de harde schijf vervolgens schoongemaakt moet worden.

Bedenk daarbij dat het verwijderen van een bestand met het DEL-commando het bestand volledig in tact laat, alleen de entry in de directory wordt verwijderd.

Dit is ook het geval met de back-up van het tekstbestand waarmee gewerkt wordt in WordPerfect. Deze back-up wordt in de meeste gevallen opgeslagen op de harddisk: na het beëindigen van WP wordt deze back-up gewist uit de directory. Middels het installatie menu van WP kan er ook voor gekozen worden dat deze back-up wordt opgeslagen op een diskette.

Ook het opnieuw formatteren van de vaste schijf verwijdert niet in alle gevallen de gegevens. Dit is alleen het geval als de schijf tevens opnieuw wordt "beschreven" met een willekeurig teken.

Samenvatting

Laat portable computers nooit onbeheerd achter, ook niet in de auto.

Zorg voor een vorm van toegangsbeveiliging (beveiligings-chip of beveiligingssoftware).

Sla op de vaste schijf alleen programmatuur op en geen gegevens.

Laat bij het verwijderen van bestanden de schijf opnieuw formatteren, waarbij gegevens overschreven worden.

Werk indien mogelijk met programmatuur waarin gegevensbestanden worden versleuteld (encryptie).

HOOFDSTUK 4

PREVENTIE: COMPUTERVIRUSSEN

òf,

Hoe loop ik 95 procent minder kans op een besmetting met een computervirus?

Er zijn vier manieren om het besmettingsgevaar zo klein mogelijk te houden:

1. Houd U aan de "Tien gouden regels voor veilig computer gebruik", die U aantreft aan het einde van dit onderwerp.

2. Gebruik virus-opsporingsprogramma´s; programma´s die kunnen vaststellen of er een besmetting heeft plaatsgevonden.

3. Gebruik preventieprogramma´s, die ten minste een bepaalde mate van bescherming bieden tegen binnen dringende virussen.

4. Gebruik hulpprogramma´s die vast kunnen stellen welke virussoort een besmetting heeft veroorzaakt en hulp kunnen bieden bij het verwijderen ervan.

Opsporingsprogramma´s kunnen op twee manieren werken. De eerste maakt een soort vingerafdruk van het systeem, waarbij de omvang van de bootsector, van de besturingssysteem-files en van alle uitvoerbare programma´s wordt opgeslagen in een logboekfile als standaard of vingerafdruk van een schoon systeem.

Als dit opsporingsprogramma daarna weer wordt gedraaid, vergelijkt het de huidige status van het systeem met de standaard in het logboekbestand. Als er verschillen zijn, kunnen die duiden op een mogelijke besmetting. Sommige uitvoerbare files kunnen b.v. groter worden, omdat een virus er zich aan heeft gehecht.

De tweede soort opsporingsprogramma's noemen we vaccinatieprograma's. Vaccinatieprogramma's duiken als het ware in Uw toepassingsprogramma's en voeren daar een zelfcontrole uit, zodat elke keer als U bijvoorbeeld Uw tekstverwerker of database gebruikt, het programma wordt gecontroleerd op een mogelijke besmetting. U krijgt een waarschuwing op Uw scherm wanneer een virus aanwezig is.

Preventieve programma's bewaken Uw systeem, waarbij ze uitkijken naar kenmerkende virusactiviteiten. De meeste virussen hechten zich bijvoorbeeld aan andere segmenten van het systeem, zoals de bootsector van een disk, om zichzelf te reproduceren.

Indien een activiteit wordt geconstateerd kan er een waarschuwing op het scherm verschijnen en het programma zal proberen het virus te beletten om een uitvoerbare file binnen te dringen.

Antivirus-programma's die een virussoort identificeren en verwijderen, brengen Uw besmettingsgevaar terug tot een minimum, door eerst de kenmerkende virusactiviteit te identificeren en daarna de code die ervoor verantwoordelijk is, te verwijderen. Deze programma's tasten het hele systeem af op zoek naar virussen. Als ze er een vinden verschijnt er een waarschuwing op het scherm die aangeeft om welke virussoort het gaat, waar die zich in het systeem bevindt en wat er gedaan moet worden om hem te vernietigen.

Waarschuwing !

Er komen echter steeds meer nieuwe virussen bij, en bestaande virussen worden voortdurend gewijzigd. Deze programma's, zoals hierboven beschreven, zijn niet altijd opgewassen tegen deze nieuwe soorten, die zich vaak zeer goed weten te beschermen en te vermommen.

De tien gouden regels voor veilig computergebruik

Het volgende beschrijft tien regels voor veilig computer gebruik. Als U zich hieraan houdt, beschermt U zichzelf tegen de grootste besmettingsgevaren van Uw systeem.

1. Plaats nooit onbekende diskettes in Uw systeem en laat ook niemand anders dat doen als U er niet zeker van bent dat die diskettes geen virussen bevatten.

2. Gebruik Uw diskettes nooit in een ander systeem zonder ze eerst te beveiligen tegen overschrijven.

3. Neem geen programma's aan als U er niet absoluut zeker van bent dat ze geen virussen bevatten. Bewaar Uw programma's en gegevens op gescheiden disketten.

4. Wees voorzichtig al U een computer huurt of als U gebruik maakt van een ander systeem.

5. Als het toch noodzakelijk is om diskettes uit te wisselen of programma's of gegevens op een vreemd systeem te draaien, pas dan een doeltreffende isolatieprocedure toe. Draai bijvoorbeeld geen potentieel besmette diskettes op Uw hoofdsysteem vooral als er een harddisk inzit. Bekijk deze programma's eerst op een onbelangrijk systeem b.v. een laptop zonder harddisk.

6. Neem geen programma's over van bulletinboards of netwerken die niet goed beheerd worden of geen voorzorgsmaatregelen nemen tegen virussen. Vraag zo nodig aan de systeembeheerder welke antivirusprocedure er wordt gevolgd.

7. Laat nooit iemand zonder toezicht gebruik maken van Uw systeem zeker niet als de kans bestaat dat er diskettes worden gebruikt door die mogelijke gast.

8. Let op onverklaarbare veranderingen in het functioneren van Uw systeem, b.v. diskdrives die zonder reden gaan werken.

9. Maak zoveel mogelijk gebruik van schrijfbeveiligingen en leg de omvang van Uw programma's ergens vast. Controleer deze aantekeningen regelmatig om te zien of er misschien veranderingen optreden die zouden kunnen duiden op een virusbesmetting.

10. Maakt regelmatig een back-up van Uw gegevens op diskette, en wel zonder programma-code. Verwijder elke besmetting op alle opslagmiddelen en draai geen back-up diskettes zonder eerst te controleren op een besmetting.